

IN THE CLAIMS

The listing of claims will replace all prior versions, and listings, of claims in the application. In the listing, claim 29 is hereby amended.

- 1 1. (Cancelled)
- 1 2. (Cancelled)
- 1 3. (Cancelled)
- 1 4. (Cancelled)
- 1 5. (Previously Presented) A computer-implemented system for protecting a
2 network, comprising:
3 a vulnerability detection system (VDS) for gathering information about the network to
4 determine vulnerabilities of a host from a plurality of hosts on the network; and
5 an intrusion detection system (IDS), cooperative with the VDS, for examining network
6 traffic responsive to the vulnerabilities of the host from the plurality of hosts as
7 determined by the VDS to detect traffic indicative of malicious activity.
- 1 6. (Previously Presented) The system of claim 5, wherein the VDS is adapted to
2 gather information about the network by sending data to the plurality of hosts and receiving
3 responsive data from the plurality of hosts.
- 1 7. (Previously Presented) The system of claim 5, wherein the VDS is adapted to
2 gather information automatically provided by the plurality of hosts.
- 1 8. (Previously Presented) The system of claim 5, further comprising:
2 a vulnerabilities rules database, in communication with the VDS, for storing rules
3 describing vulnerabilities of the plurality of hosts,
4 wherein the VDS is adapted to analyze the gathered information with the rules to
5 determine the vulnerabilities of the plurality of hosts.

1 9. (Previously Presented) The system of claim 8, wherein the VDS is adapted to
2 analyze the gathered information with the rules to identify operating systems on the plurality of
3 hosts and determine the vulnerabilities responsive to the respective operating systems.

1 10. (Previously Presented) The system of claim 8, wherein the VDS is adapted to
2 analyze the gathered information with the rules to identify open ports on the plurality of hosts
3 and determine the vulnerabilities based on the open ports.

1 11. (Previously Presented) The system of claim 8, wherein the VDS is adapted to
2 analyze the gathered information with the rules to identify applications executing on the plurality
3 of hosts and determine the vulnerabilities based on the applications.

1 12. (Original) The system of claim 5, further comprising:
2 an intrusion rules database, in communication with the IDS, for storing rules describing
3 malicious activity,
4 wherein the IDS is adapted to analyze the network traffic with the rules to detect network
5 traffic indicative of exploitations of the determined vulnerabilities.

1 13. (Original) The system of claim 5, wherein the IDS is adapted to detect traffic
2 indicative of exploitations of only the determined vulnerabilities.

1 14. (Cancelled)

1 15. (Original) The system of claim 5, wherein the VDS is adapted to update the
2 determined vulnerabilities, and wherein the IDS is adapted to detect traffic indicative of
3 malicious activity in response to the update.

1 16. (Original) The system of claim 15, wherein the VDS is adapted to update the
2 determined vulnerabilities in response to a change in the network.

1 17. (Previously Presented) A computer-implemented method for protecting a
2 network, comprising:
3 gathering information about the network to determine vulnerabilities of a host from a
4 plurality of hosts on the network; and
5 cooperative with the step of gathering information, examining network traffic responsive
6 to the determined vulnerabilities of the host from the plurality of hosts to detect
7 network traffic indicative of malicious activity.

1 18. (Previously Presented) The method of claim 17, wherein gathering information
2 comprises sending data to plurality of hosts on the network and receiving responsive data from
3 the plurality of hosts.

1 19. (Previously Presented) The method of claim 17, wherein gathering information
2 comprises receiving data automatically provided by the plurality of hosts on the network.

1 20. (Previously Presented) The method of claim 17, further comprising:
2 storing rules to describe vulnerabilities of the plurality of hosts,
3 wherein determining vulnerabilities includes analyzing the gathered information with the
4 rules.

1 21. (Previously Presented) The method of claim 20, wherein determining
2 vulnerabilities comprises analyzing the gathered information with the rules to identify operating
3 systems on the plurality of hosts.

1 22. (Previously Presented) The method of claim 20, wherein determining
2 vulnerabilities comprises analyzing the gathered information with the rules to identify open ports
3 on the plurality of hosts.

1 23. (Previously Presented) The method of claim 20, wherein determining
2 vulnerabilities comprises comparing the gathered information against the rules to identify
3 applications on the plurality of hosts.

1 24. (Original) The method of claim 17, further comprising:
2 storing rules describing malicious activity,
3 wherein detecting network traffic indicative of malicious activity comprises analyzing the
4 network traffic with the rules to detect traffic indicative of exploitations of the
5 determined vulnerabilities.

1 25. (Original) The method of claim 17, wherein examining network traffic consists of
2 detecting traffic indicative of exploitations of only the determined vulnerabilities.

1 26. (Cancelled)

1 27. (Previously Presented) The method of claim 17, further comprising:
2 updating the determined vulnerabilities and detecting traffic indicative of malicious
3 activity in response to the update.

1 28. (Original) The method of claim 27, wherein the updating is responsive to a
2 change in the network.

1 29. (Currently Amended) A computer program product, comprising:
2 a computer-readable medium having computer program logic embodied therein for
3 protecting a network, the computer program logic:
4 gathering information about the network to determine vulnerabilities of a host from a
5 plurality of hosts on the network; and
6 cooperative with the step of gathering information, examining network traffic responsive
7 to the determined vulnerabilities of the host from the plurality of hosts to detect
8 network traffic indicative of malicious activity.

1 30. (Previously Presented) The computer program product of claim 29, wherein
2 gathering information comprises sending data to plurality of hosts on the network and receiving
3 responsive data from the plurality of hosts.

1 31. (Previously Presented) The computer program product of claim 29, wherein
2 gathering information comprises receiving data automatically provided by the plurality of hosts
3 on the network.

1 32. (Previously Presented) The computer program product of claim 29, further
2 comprising:
3 storing rules to describe vulnerabilities of the plurality of hosts,
4 wherein determining vulnerabilities includes analyzing the gathered information with the
5 rules.

1 33. (Previously Presented) The computer program product of claim 32, wherein
2 determining vulnerabilities comprises analyzing the gathered information with the rules to
3 identify operating systems on the plurality of hosts.

1 34. (Previously Presented) The computer program product of claim 32, wherein
2 determining vulnerabilities comprises analyzing the gathered information with the rules to
3 identify open ports on the plurality of hosts.

1 35. (Previously Presented) The computer program product of claim 32, wherein
2 determining vulnerabilities comprises comparing the gathered information against the rules to
3 identify applications on the plurality of hosts.

1 36. (Original) The computer program product of claim 29, further comprising:
2 storing rules describing malicious activity,
3 wherein detecting network traffic indicative of malicious activity comprises analyzing the
4 network traffic with the rules to detect traffic indicative of exploitations of the
5 determined vulnerabilities.

1 37. (Original) The computer program product of claim 29, wherein examining
2 network traffic consists of detecting traffic indicative of exploitations of only the verified
3 vulnerabilities.

1 38. (Cancelled)

1 39. (Previously Presented) The computer program product of claim 29, further
2 comprising:

3 updating the determined vulnerabilities; and

4 detecting traffic indicative of malicious activity in response to the update.

1 40. (Previously Presented) The computer program product of claim 39, wherein the
2 updating is responsive to a change in the network.